IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of Melissa W. Dunn Art Unit 2154
Serial No. 10/084,859
Filed February 27, 2002
Confirmation No. 8746
For SYSTEM AND METHOD FOR USER-CENTRIC AUTHORIZATION TO ACCESS USER-SPECIFIC INFORMATION
Examiner Joshua Joo

APPEAL BRIEF

Frank Agovino, Reg. No. 27,416
SENNIGER POWERS
One Metropolitan Square, 16th Floor
St. Louis, Missouri 63102
(314) 231-5400

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

REFERENCES

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of Melissa W. Dunn Art Unit 2154
Serial No. 10/084,859
Filed February 27, 2002
Confirmation No. 8746
For SYSTEM AND METHOD FOR USER-CENTRIC AUTHORIZATION TO ACCESS USER-SPECIFIC INFORMATION
Examiner Joshua Joo

May 21, 2007

APPEAL BRIEF

This is an appeal from the final rejection of the claims of the above-referenced application made in the Final Office action dated **November 30, 2006.** A Notice of Appeal was filed on **April 13, 2007.**

The appeal brief fee in the amount of $500.00 is submitted herewith.

I. REAL PARTY IN INTEREST

The real party in interest in connection with the present appeal is Microsoft Corporation of One Microsoft Way, Redmond, Washington, 98052, a corporation of the state of Washington, owner of 100 percent interest in the pending application.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any pending appeals or interferences which may be related to, directly affect or be directly affected by, or have a bearing on, the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 3, 5, 6, 9-13, 15-19, 21, 29, 30, and 32-37, as set forth in the Claims Appendix, are currently pending in the application for consideration. Claims 1, 2, 4, 7, 8, 14, 20, 22-28, 31 and 38-46 have been canceled.

Claims 3, 5, 6, 9-13, 15-19, 21, 29, 30, and 32-37 stand rejected. The rejection of independent claims 15 and 29 is being appealed.

IV. STATUS OF AMENDMENTS

No amendments have been filed after the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following summary correlates claim elements to embodiments described in the application specification, but does not in any manner limit claim interpretation. Rather, the following summary is provided only to facilitate the Board's understanding of the subject matter of this appeal.

According to aspects of the present invention, web-services users 202 control access to their user-specific information stored with a web-services service by access control settings. The web-services client determines dynamically whether to grant or deny an access request that does not comply with default access control settings. Advantageously, the present invention rests the burden of managing intentions with each web-services client. Stated differently, the present invention places no additional burdens on the authorization and authentication mechanisms used by the web-services provider. *See* Application, pages 16-22, 41 (lines 8-20) and FIG. 2.

In this regard, claim 29 is directed to a system for controlling access to user-specific information in a network computing environment. As described in the application and illustrated in FIG. 2, aspects of the invention include a web-services service provider 204, a user 202 of a service (#1 to #n) of the web-services provider 204, a client 220 of the web-services provider 204, an access control engine 232 and a consent engine 236. The web-services provider 204 maintains a data store of user-specific information associated with the user 202. The user-specific information is accessible by the user 202. Accessed by the client 220 is controlled by the user 202. A set of default access preferences 234 define a list of default access permissions 210, 216 that are allowed by the user 202.

The client 220 generates a request to access to certain of the user-specific information associated with the user 202. The request identifies an intended use by the client 220 of the certain user-specific information in the data store.

The access control engine 232 receives the client request to access the certain user-specific information and dynamically creates an access control rule by comparing the set of default access preferences with the intended use by the client. The access control rule grants the requested access by the client to the certain user-specific information if the intended use of the client of the certain user-specific information is within the list of default access permissions defined by the set of default access preferences defined by the user 202.

The consent engine 236 generates an option list in response to the client's request for user-specific information when the intended use is outside the list of default access preferences defined by the user 202. The option list contains at least one entry based on the intended use by the client of the user-specific information in the data store. The consent engine 236 displays on the display interface of the network communication device an option menu reflecting the generated option list. The option menu prompts the user to accept or reject at least one option displayed on the option menu using the selection interface of the network communication device. *See* Application, pages 34, 35 and FIGS. 5A, 5B.

Claim 15 is directed to a method of controlling access to user specific information for use in a network computer system including a web-services provider, a user of a service provided by the web-services provider, and a client of the web-services provider. The web-services provider receives a request from the client to access the certain user-specific information in the data store of user-specific information associated with the user. The user-specific information is accessible by the client controlled by the user. The client generates an intended use request to certain user-specific information in the data store. The web-services provider determines an allowed level of access permitted by the user and compares the generated intended use request with the determined allowed level of access. If the generated intended use request is outside the allowed level of access, a consent engine is invoked. The consent engine informs the user of the client's request to access the certain user-specific information in the data store and invites the user to permit or to deny the client's request to access the certain user-specific information. When the generated intended use request by said client of the certain user-specific information is within the determined allowed level of access permitted by the user, the web-services provider completes the request from the client to access the certain user-specific information in the data store.

As further illustrated in FIG. 7 and the corresponding descriptions in specification, such as page 41, embodiments of the invention places the burden of managing intentions on each web-

services client. This advantage places no additional burdens on the authorization and authentication mechanisms used by the web-services provider and a separate service-side fabric is not required

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Appellant appeals the rejections of claims 5, 15, 19, 21, 29-30 and 32-37 under 35 U.S.C. §102(b) as being anticipated by U.S. Pub. App. 2003/0191703 (Chen et al.).

VII. ARGUMENT

A claim is anticipated only if each and every element as set forth in the claim is disclosed, either expressly or inherently in a single prior art reference.[1] Applicants submit that each and every element as set forth in the recited claims is not found, either expressly or inherently in the Chen et al. reference. Thus, the Chen et al. reference does not anticipate the claims.

A. Claim 15

Claim 15 is directed to a method of controlling access to user specific information for use in a network computer system including a web-services provider, a user of a service provided by the web-services provider, and a client of the web-services provider.

Claim 15 is submitted to be unanticipated by and patentable over Chen et al. in that the reference fails to disclose or teach "**generating an intended use request** by the client of the certain user-specific information in the data store" and "**comparing the generated intended use request with the determined allowed level of access**." Second, Chen et al. fails to disclose or teach "**invoking a consent engine in response to the client's request** if the generated intended use request is outside the allowed level of access, said consent engine informing the user of the client's request to access the certain user-specific information in the data store and inviting the user to permit or to deny the client's request to access the certain user-specific information in the data store."

[1] M.P.E.P. § 2131. *See also Schering Corp. v. Geneva Pharmaceuticals*, 339 F.3d 1373, 1379 (Fed. Cir. 2003) (citing *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987)).

1. Summary of Chen et al.

Chen et al. teaches a system for providing aggregated accounts information to an interested third party. (Chen et al., Abstract). The client is allowed to specify various levels of access permissions for an interested party to control the level of detail accessible to one or more interested parties. (Chen et al., Abstract). However, the client grants access by the interested party and not the intended use of the information by the interested party. In particular, in paragraph 148, Chen et al. discloses the client investor is allowed to "control or change the accounts, if any that are accessible by a particular interested party using the data aggregation system." Furthermore, the client investor may choose "one or more interested parties, or interested party team, who may access client investment account information, as well as the option of specifying the level of detail available to each interested party." (Chen et al., pages 14-15, paragraph 148). Specifically, "the data aggregation system will only display a client's account data to an interested party if and when the client so allows." (Chen et al., pages 14-15, paragraph 148). Chen et al. teaches that "[T]the methods and techniques by which the data aggregation system allows a client to manage access to his account information by interested parties is referred to herein as permissioning." (Chen et al., pages 14-15, paragraph 148). In other words, Chen et al. teaches nothing more than allowing a client investor the ability to grant permission to one or more interested parties to access the client investor's aggregated accounts information and the permission is granted on the basis of who the interested party is and not the interested party's use of the information as recited in the claimed invention.

2. Response to Examiner's Arguments

The final Office action takes the position that Chen et al. teaches both generating an intended use request by the client of the certain user-specific information in the data store and invoking a consent in response the client's request if the generated intended user request is outside the allow level of access. The Office points to paragraph 138 of Chen et al. as teaching generating an intended use request by the client of the certain user-specific information in the data store. However the Examiner admits that Chen et al. just teaches a login request comprising a name, id and password. The login request does not include request for certain user-specific information. Additionally, access is granted based on the level of the data, aggregate or detail, not the intended use of data as claimed in claim 15.

For example, FIG. 14 of Chen et al. illustrates a client permissions report 1400. The client permissions report 1400, described in paragraph [0163], may include a list of the aggregated accounts 1405 associated with the requesting client user and an identification of each interested party 1410 to whom account access is provided. For each listed aggregated account, the client permissions report 1400 may include a descriptive entry indicating the level of access 1415 currently provided for each listed interested party 1410 for that account 1405. For example, if the client user has a financial advisor, then client permissions report 1400 may include a list of the client accounts 1405 which the requesting financial advisor is authorized to view using the data aggregation system. The listed accessible accounts 1405 may include external investment accounts which the client(s) maintains at one or more external account providers, as well as internal accounts maintained by an account provider associated with the data aggregation system.

Furthermore, in paragraphs [0164-0168], Chen et al. teaches 4 access levels: (1) a summary level in which an interested party 1410 may view only the total account value or balance for each internal and external account for the associated investment account category, as well as the aggregated total account value; (2) an account detail level view report 1500 (illustrated in FIG. 15) may be provided in which an interested party 1410 may view the account balance or value information provided with the summary level in addition to account transaction details information (e.g., bought and sold security, date, and price); (3) a transactions detail level view which includes account transaction details information such as, but not limited to, purchases made, charges, credits, and payments; and (4) a no access level which prohibits any interested party 1410 from having access to the associated aggregated account 1405 (e.g., "No access"). Determining an access for an interested party is not the same as determining the intended use of the requested information.

Additionally, the Office points to paragraph 171, 175 and 176 as invoking a consent in response the client's request if the generated intended user request is outside the allow level of access. Applicant respectfully disagrees. Paragraphs 171, 175, and 176 teach allowing the user to select names to set permissions. The server provides a list of potential interested parties whom the client may choose to grant account access. However, this list is not generated based on a request of the interested party as recited in the claim 15. For example, in paragraph 175 Chen et al. teaches that the list is the current set of **all** interested parties and in paragraph 176 the

list is based on the **interested parties previously entered or selected by the user**. The list is not based on an indented use originated by the interested party nor is it generated in response to a request for certain user-specific information as recited in claim 15.

3. Generating an Intended Use Request by the Client and Comparing the Generated Intended Use Request

In contrast to Chen et al., the present invention as recited in claims 15 includes "**generating an intended use request** by the client of the certain user-specific information in the data store" and "**comparing the determined intended use request** with the determined allowed level of access." Pages 68-69 of the present application illustrates an example where Joe goes to a financial web site which customizes the pages it displays to include the user's name and items of local financial news of interest to the user. After reviewing the options, Joe decides to subscribe to the financial advisor web site. The site allows Joe to enter a series of stock symbols and industry types (e.g. tech sector) in which he is interested. The financial web site advisors will send Joe email when something of interest happens in any of the entered industry types. Additionally, the site will send an email alert to Joe when there are marked changes in the value of stocks listed in Joe's entered portfolio. After making his selections, Joe is asked to grant permission for the financial web site to contact him via email and alerts. The financial web site includes verbiage indicating that Joe agreeing to get email and alerts from the financial web site does not mean that the site will send him any other type of email or alert. Joe agrees and starts filling in the required information not available in his web-services.

Accordingly, if something of interest has occurred in one of the industry types selected by Joe, the financial web site will send a query request against Joe's profile using the task ID and intentions for notifying Joe that something of interest occurred in a selected industry type. In this case, the financial web site will be allowed to access Joe's email address to send an email notifying Joe of the event. Now suppose the financial web site sends a query request against Joe's profile using the task ID and intentions for advertising. Because Joe has not allowed the site access to his email address for the intention of sending an advertisement, the consent system displays the information and intentions to Joe on a consent menu. If Joe agrees, the consent system writes a financial web site specific role into Joe's profile access control list that includes

the advertising intention. If Joe does not agree, the financial web site will not be allowed to access Joe's email address to send the advertisement.

Therefore, Joe not only specifies who (e.g., the financial web site) is allowed access to his personal information but the intention of the use of the information (e.g. when a sector has something interesting happening, when there are marked changes in the value of stocks listed in Joe's portfolio, or for targeting content and advertising). Furthermore, the permission is conditioned on the financial web site's intentions. From the example above, the financial web site can access Joe's email address when it intents to send Joe an email when a something interesting is happening within a selected industry sector. On the other hand, the financial web site can not access Joe's email address when it intents to send Joe an advertisement.

Nothing in Chen et al. teaches, suggests or makes obvious comparing the generated intended use request with the determined allowed level of access. The Office's reliance on paragraph 139 of Chen et al. is misplaced; it teaches nothing more than providing the interested party with a list of client accounts accessible to the interested party if the interested party's identification/authentication information is valid. (Chen et al., page 14, paragraph 139).

Thus, Chen et al. fails to teach **comparing the generated intended** use request with the determined allowed level of access as recited in claims 15.

4. Invoking a Consent Engine

With respect to invoking a consent engine, the present invention as recited in claims 15 includes "**invoking a consent engine** in response to the client's request if the generated intended use request is outside the allowed level of access, said consent engine informing the user of the client's request to access the certain user-specific information in the data store and inviting the user to permit or to deny the client's request to access the certain user-specific information in the data store." (Specification, page 19, lines 25-30).

An exemplary consent menu is illustrated in FIG. 3. For example, the access control engine 232 generates a list of options to present to user 202 in a consent menu format on a display associated with the end user's network communication device. (Specification, page 19, lines 14-17). The access request identifies the reason why web-services client system 220 desires access (e.g., to complete an on-line sale) and the consent options are determined from the client's access request. (Specification, page 19, lines 17-22). The consent options also identify

the type of information desired (e.g., demographic information 206), and/or the intended method of access (e.g., read only, read/write, and the like). (Specification, page 19, lines 22-24). The consent menu is presented to user 202 and prompts user 202 to authorize or deny the client's access request. (Specification, page 19, lines 25-26). If user 202 authorizes the request, access control engine 232 writes an appropriate access rule (line 240) to the access control list associated with the particular user-specific information requested (e.g., access control list 210). (Specification, page 19, lines 26-29). If user 202 denies the request, access control engine 232 sends a message to web-services client system 220 denying the requested access. (Specification, page 19, lines 29-30).

Nothing in Chen et al. teaches, suggests or anticipates **invoking a consent engine to inform the user of the client's request to access user-specific information and its intended use** and inviting the user to permit or to deny the client's request to access the information as recited in the claims. In fact, Chen et al. teaches the away from such an approach. Chen et al. discloses the list of potential interested parties are provided by the application server. (Chen et al., page 17, paragraph 175). Furthermore, Chen et al. teaches the application server maintains and stores the list of potential interested parties "based upon the interested parties previously entered or selected by the client user for other aggregated accounts". (Chen et al., page 18, paragraph 176).

For these reasons, claim 15 is submitted to be unanticipated by and patentable over Chen et al. et al. Claims 16-19 and 21 depend directly or indirectly from claim 15 and are submitted to be patentable over Chen et al. for at least the same reasons as claim 15.

B. Claim 29

Independent claim 29 is directed to a system for controlling access to user-specific information in a network computing environment.

Claim 29 is submitted to be unanticipated by and patentable over Chen et al. for substantially the same reasons as claim 15. That is Chen et al. fails to disclose or teach a web-services provider system including "**a request** to access certain of the user-specific information associated with the user, said request **identifying an intended use by the client of the certain user-specific information** in the data store." Second, Chen et al. fails to disclose or teach such a system including "**a consent engine generating an option** list in response to the client's request

for user-specific information having at least one entry therein **based on the intended use by the client** of the user-specific information in the data store."

1. Request Identifying an Intended Use by the Client of the Certain User-Specific Information

As explained in the example above, Joe not only specifies who (e.g., the financial web site) is allowed access to his personal information but the intention of the use of the information (e.g. when a sector has something interesting happening, when there are marked changes in the value of stocks listed in Joe's portfolio, or for targeting content and advertising). Furthermore, the permission is conditioned on the financial web site's intentions. From the example above, the financial web site can access Joe's email address when it intents to send Joe an email when a something interesting is happening within a selected industry sector. On the other hand, the financial web site can not access Joe's email address when it intents to send Joe an advertisement.

Nothing in Chen et al. teaches, suggests or makes obvious **a request** to access certain of the user-specific information associated with the user, said request **identifying an intended use by the client of the certain user-specific information** in the data store. The Office's reliance on paragraph 138 of Chen et al. is misplaced; by the Examiner's own admission it teaches nothing more than the login of the interested party. (Chen et al., page 14, paragraph 138). Chen et al. cannot anticipate claim 29 because it fails to teach, suggest or makes obvious the request **identifying an intended use by the client of the certain user-specific information** as recited in the claim. Thus, Chen et al. fails to teach comparing the generated intended use request with the determined allowed level of access as recited in claims 29.

2. Consent engine

With respect the consent engine, the present invention as recited in claim 2 includes "**a consent engine generating an option list in response to the client's request for user-specific information having at least one entry therein based on the intended use by the client of the user-specific information** in the data store." (Specification, page 19, lines 25-30).

As explained above, nothing in Chen et al. teaches, suggests or anticipates **a consent engine generating an option list in response to the client's request for user-specific**

information having at least one entry therein based on the intended use by the client of the user-specific information as recited in the claims. In fact, Chen et al. teaches the away from such an approach and has no need or purpose for a consent engine. Chen et al. discloses the list of potential interested parties are provided by the application server. (Chen et al., page 17, paragraph 175). Furthermore, Chen et al. teaches the application server maintains and stores the list of potential interested parties "based upon the interested parties previously entered or selected by the client user for other aggregated accounts". (Chen et al., page 18, paragraph 176).

For at least the reasons stated above, claim 29 is submitted to be unanticipated by and patentable over Chen et al. et al. Claims 3, 5, 6, 9-13, 30, and 32-37 depend directly of indirectly from claim 29 and are submitted to patentable over Chen et al. for at least the reasons as claim 29.

VIII. CONCLUSION

For the reasons stated above, appellant respectfully requests that the Office's rejections be reversed and that claims 1-33, 35, 36, 38, 40, 41, 46, 47 and 49-58 be allowed.

Respectfully submitted,

/Frank R. Agovino/

Frank R. Agovino, Reg. No. 27,416
SENNIGER POWERS
One Metropolitan Square, 16th Floor
St. Louis, Missouri 63102
(314) 231-5400

FRA/BAW/cjl

IX. CLAIMS APPENDIX

Claim 1-2. (canceled)

Claim 3. (previously presented) The system of claim 29 wherein the client's request to access the certain user-specific information in the data store identifies a desired subject matter to be accessed and a method of accessing the desired subject matter and wherein comparing the set of default access preferences with the intended use by the client further comprises determining if the set of default access preferences permits the client to access the desired subject matter; and determining if the set of default access preferences permits the identified method of accessing the desired subject matter.

Claim 4. (canceled)

Claim 5. (previously presented) The system of claim 32 wherein creating the access control rule comprises updating a list of access permissions such that said list of access permissions reflects whether the user accepted or rejected the at least one option.

Claim 6. (previously presented) The system of claim 29 wherein the client determining if the client has a local copy of the certain user-specific information in the data store before transmitting the request, the client retrieving said local copy of the certain user-specific information if the local copy is available, the client determining if said local copy of the certain user-specific information is current and transmitting the request only if said local copy of the certain user-specific information is not available and not current.

Claim 7-8. (canceled)

Claim 9. (previously presented) The system of claim 29 wherein the access control engine determining if the client has an access subscription right to the certain user-specific information in the data store and the access control engine permitting the client to have access to the certain user-specific information in the data store if the client has the access subscription right to the certain user-specific information in the data store.

Claim 10. (previously presented) The system of claim 29 wherein the client identifying a requested form of access to the user-specific information in the data store and the access control engine granting the requested access to the certain user-specific information in the data store if the user has granted said form of access requested by the client comprises permitting the client to read the requested user-specific information in the data store and permitting the client to write the requested user-specific information in the data store.

Claim 11. (previously presented) The system of claim 10 wherein permitting the client to read the requested user-specific information in the data store comprises accessing said certain user-specific information and transmitting a copy of the accessed certain user-specific information to the client in a SOAP message.

Claim 12. (previously presented) The system of claim 10 wherein permitting the client to write the certain user-specific information in the data store comprises receiving at the web-services provider a SOAP message from the client identifying the certain user-specific information and writing the identified certain user-specific information in the data store.

Claim 13. (previously presented) The system of claim 29 wherein creating the access control rule to permit the client to have access to the certain user-specific information in the data store if the default access permissions permits the identified intended use comprises creating the access control rule to permit the client to read the certain user-specific information in the data store and creating the access control rule to permit the client to write the certain user-specific information in the data store.

Claim 14. (canceled)

Claim 15. (previously presented) A method of controlling access to user specific information for use in a network computer system including a web-services provider, a user of a service provided by the web-services provider, and a client of the web-services provider, said method of controlling access to the user-specific information comprising:

operatively receiving at the web-services provider a request from the client to access the certain user-specific information in the data store wherein the web-services provider maintaining a data store of user-specific information associated with the user, said user-specific information accessible by the user and having access by the client controlled by the user, said client seeking access to certain of the user-specific information in the data store;

generating an intended use request by the client of the certain user-specific information in the data store;

determining an allowed level of access permitted by the user;

comparing the generated intended use request with the determined allowed level of access;

invoking a consent engine in response to the client's request if the generated intended use request is outside the allowed level of access, said consent engine informing the user of the client's request to access the certain user-specific information in the data store and inviting the user to permit or to deny the client's request to access the certain user-specific information in the data store; and

completing the request from the client to access the certain user-specific information in the data store when the generated intended use request by said client of the certain user-specific information is within the determined allowed level of access permitted by the user.

Claim 16. (previously presented) The method of claim 15 wherein generating the intended use request by the client of the certain user-specific information in the data store comprises:

determining a type of information within the certain user-specific information in the data store that is being requested by the client; and

determining a form of access to the certain user-specific information in the data store that is being requested by the client.

Claim 17. (previously presented) The method of claim 16 wherein comparing the generated intended use request with the determined allowed level of access comprises:

determining if the user permits access to the type of information within the certain user-specific information in the data store that is being requested by the client; and

determining if the user permits the form of access to the certain user-specific information in the data store that is being requested by the client.

Claim 18. (previously presented) The method of claim 17 further comprising:

creating an access filter, said access filter defining an extent to which the user permits access to the type of information within the certain user-specific information in the data store and an extent to which the user permits the form of access to the user-specific information in the data store; and

wherein completing the request from the client to access the certain user-specific information in the data store when the generated intended use request is within the determined allowed level of access further comprises:

applying the access filter to the certain user-specific information in the data store to create a filtered information set; and

permitting the client to access the filtered information set.

Claim 19. (previously presented) The method of claim 15 further comprising denying the client access to the requested certain user-specific information in the data store if the determined intended use is outside the allowed level of access.

Claim 20. (canceled)

Claim 21. (original) One or more computer-readable media having computer-executable instructions for performing the method recited in claim 15.

Claim 22-28. (canceled)

Claim 29. (previously presented) A system for controlling access to user-specific information in a network computing environment, the system comprising:

a web-services service provider;

a user of a service of the web-services provider, the web-services provider maintaining a data store of user-specific information associated with the user, said user-specific information accessible by the user and having access by the client controlled by the user, and a set of default access preferences defining a list of default access permissions allowed by the user;

a client of the web-services provider, said client generating a request to access to certain of the user-specific information associated with the user said request identifying an intended use by the client of the certain user-specific information in the data store;

an access control engine operatively receiving the client request to access the certain user-specific information and dynamically creating an access control rule by comparing the set of default access preferences with the intended use by the client, said access control rule granting the requested access by the client to the certain user-specific information when the intended use of the client of the certain user-specific information is within the list of default access permissions defined by the set of default access preferences allowed by the user; and

a consent engine generating an option list in response to the client's request for user-specific information having at least one entry therein based on the intended use by the client of the user-specific information in the data store, said consent engine displaying on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option displayed on the option menu using the selection interface of the network communication device.

Claim 30. (original) The system of claim 29 further comprising a network communication device having a display interface and a selection menu and wherein the user communicates with the web-services provider via the network communication device.

Claim 31. (canceled)

Claim 32. (previously presented) The system of claim 29 wherein the network communication device generates a selection signal indicative of whether the user accepted or rejected the at least one option displayed on the option menu.

Claim 33. (previously presented) The system of claim 29 wherein the consent engine provides a consent signal having a parameter indicative of whether the user accepted or rejected the at least one option and wherein the access control engine receives the consent signal, said access control engine granting the requested access if the consent signal indicates that the user accepted the at least one option.

Claim 34. (original) The system of claim 33 wherein the access control engine denies the requested access if the consent signal indicates that the user rejected the at least one option.

Claim 35. (original) The system of claim 29 further comprising an authentication engine authenticating a digital identity of the user and wherein the access control engine denies the requested access if the digital identity of the user is not authenticated by the authentication engine.

Claim 36. (original) The system of claim 29 further comprising a client intentions document identifying the intended use by the client of the user-specific information in the data store.

Claim 37. (original) The system of claim 36 further comprising:

a network communication device having a display interface and a selection menu and wherein the user communicates with the web-services provider via the network communication device; and

a consent engine retrieving the client intentions document and generating an option list having at least one entry therein based on the intended use identified in the intentions document, said consent engine displaying on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option displayed on the option menu using the selection interface of the network communication device.

Claim 38-46. (canceled)

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.